Industrial
Cellular VPN Router

IR-711UB User's Manual

Version 1.2
March, 2010.

ORing Industrial Networking Corp.
4F, NO.3, Lane 235, Baociao Rd. Sindian City,
Taipei County 23145 Taiwan, R.O.C.
Tel: + 886 2 2918 3036
Fax: + 886 2 2918 3084
Website: www.oring-networking.com
E-mail: support@oring-networking.com

Tables of Content

Getting to Know your Wireless VPN router 1

1.1 Overview 1

1.2 Software Features 1

1.3 Hardware Features 1

Hardware Overview 2

3.1 Front Panel 2

3.2 Front Panel LEDs 3

Cables and Antenna 4

4.1 Ethernet Cables 4

Management Interface 6

5.1 First-time Installation 6

5.2 Main Interface 8

5.3.1 Basic Setting 9

WAN 9

LAN 10

DHCP 10

NAT Setting 12

Security Setting 16

VPN Setting 18

Routing Protocol (Routing Setting) 25

Miscellaneous (DDNS) 28

5.3.2 System Tools 29

Date & Time 29

System Event 30

Login Setting 30

Router Restart 31

Firmware Upgrade 32

Save/Restore Configurations 33

Remote Management 34

Miscellaneous (Ping) 34

5.3.3 System Status 35

System Info 35

System Log 35

Traffic Statistics 36

Technical Specifications 37

Appendix A 38
How to configure openvpn and use openvpn in the Windows? 38

Getting to Know your Wireless VPN router

1.1 Overview

IR-711UB is a reliable VPN Router with 1 port 10/100T(X) port and 1 port USB 2.0 port. It could be configured to operate in Modem (56K/GPRS/3G/3.5G Modem) dial up. In the mode of Modem dial up, it support both traditional 56K modem and GPRSG/3G/3.5G Modem with USB interface, that can provide local LAN connect to internet through USB modem. Therefore, IR-711UB is one of the best solutions for applications of Internet communication.

1.2 Software Features

- Intuitive Web-based management user interface for simply and easily operation.
- USB connectivity providing Internet access via the USB to RS232 convertor + modem or 3G HSDPA module (HUAWEI E220) directly.
- Functions of firewall provides many security features such as blocking attacks from hacker, especially IP Spoofing, Ping flood, Ping of Death, DOS, DRDOS, Stealth Scan, ICMP flooding etc.
- Advanced firewall configuration to extend the capability and security, such as Virtual Server, Port Trigger, DMZ host, UPnP auto Forwarding, IP Filter and MAC filter.

1.3 Hardware Features

- 10/100Base-T(X) Ethernet ports for LAN connection individually.
- Power Inputs: 12~48 VDC on terminal block
- Casing: IP-30
- Dimensions(W x D x H) : 70mm(W)x26mm(D)x95mm(H)
- Operating Temperature: -20 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing

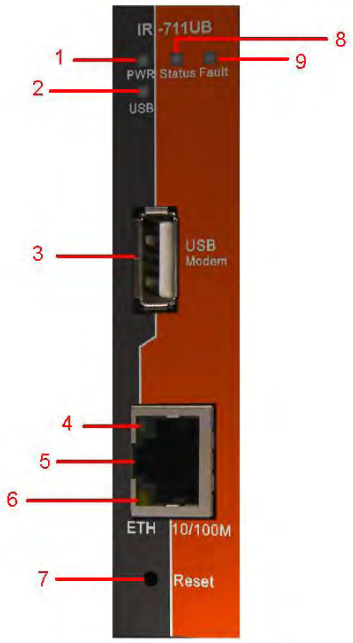
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IR-711UB.

Port	Description
10/100 RJ-45 fast Ethernet ports	10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto

IR-711UB



1. LED for PWR. When the PWR links, the green led will be light on.
2. LED for USB modem status
3. USB port for 3G USB modem connection LED for Ethernet ports link status.
4. LED for Ethernet port active.
5. 10/100Base-T(X) RJ-45 fast Ethernet ports
6. LED for Ethernet ports speed.
7. Reset button. Push the button 5 seconds for factory default.
8. LED for Status. When the system is ready, the green led will be light on.
9. LED for Fault Relay. When the fault occurs, the amber LED will be light on.

3.2 Front Panel LEDs

LED	Color	Status	Description
System LED			
PWR	Green	Green On	DC power activated.
STATUS	Green	Green On	Power is on and booting up
		Green blinking	Booting up
Fault	Amber	Blinking	Fault occur by fault setting
USB Status	Green	On	Modem Ready
		Blinking	Modem Connecting
10/100Base-T(X) Fast Ethernet ports			
Amber	On	Port link up at 100Mbps.	
	Off	Port link up at 10Mbps.	
Green	Blinking	Data transmitted.	

Cables and Antenna

4.1 Ethernet Cables

The IR-711UB VPN routers have standard Ethernet ports. According to the link type, the routers use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The IR-711UB routers support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and router. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment

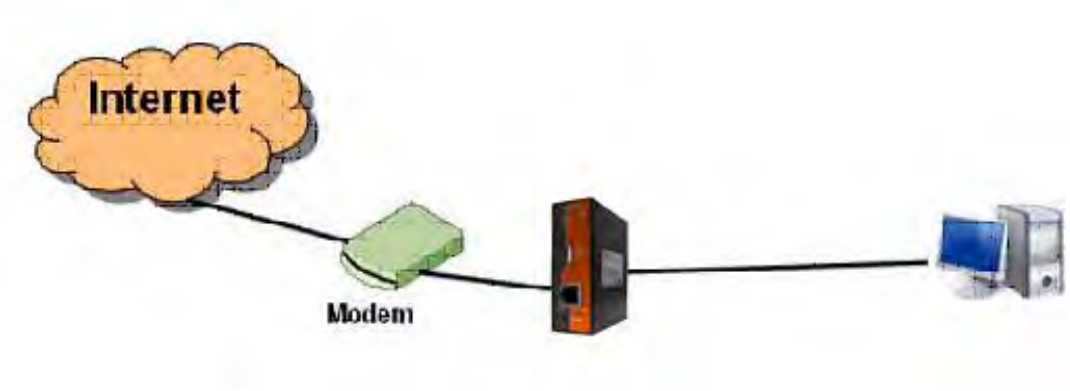
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Management Interface

5.1 First-time Installation

Before installing IR-711UB VPN router, you need to access the router by a computer equipped with an Ethernet card or wireless LAN interface. Using an Ethernet card to connect to LAN port is easier and recommended.



Basic connection for IR-711UB

Step 1: Select the Power Source

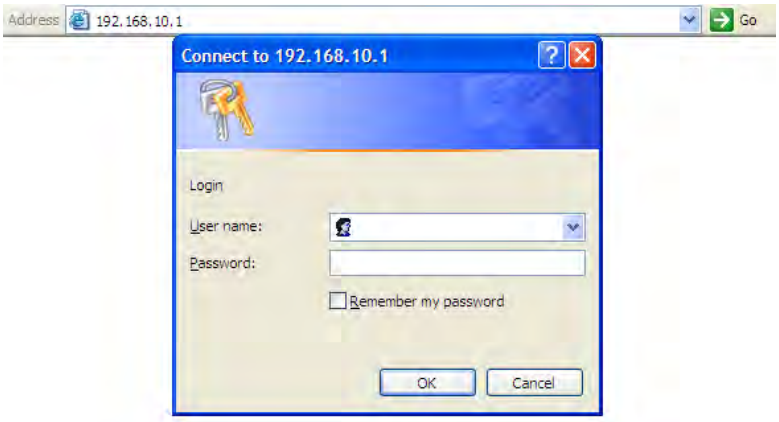
IR-711UB VPN Router can be powered by +12~48V DC power input,

Step 2: Connect a computer to IR-711UB

Use either a straight-through Ethernet cable or cross-over cable to connect to ETH1 of IR-711UB router to a computer. If the LED of the LAN port lights up, it indicates the connection is established. After that, the computer will initiate a DHCP request to get an IP address from the router.

Step 3: Use the web-based manager to configure IR-711UB

The default gateway IP of IR-711UB router is 192.168.10.1. Start the web browser of your computer and type http://192.168.10.1 in the address box to access the webpage. A login window will popup, and then enter the default login name **admin** and password **admin.**



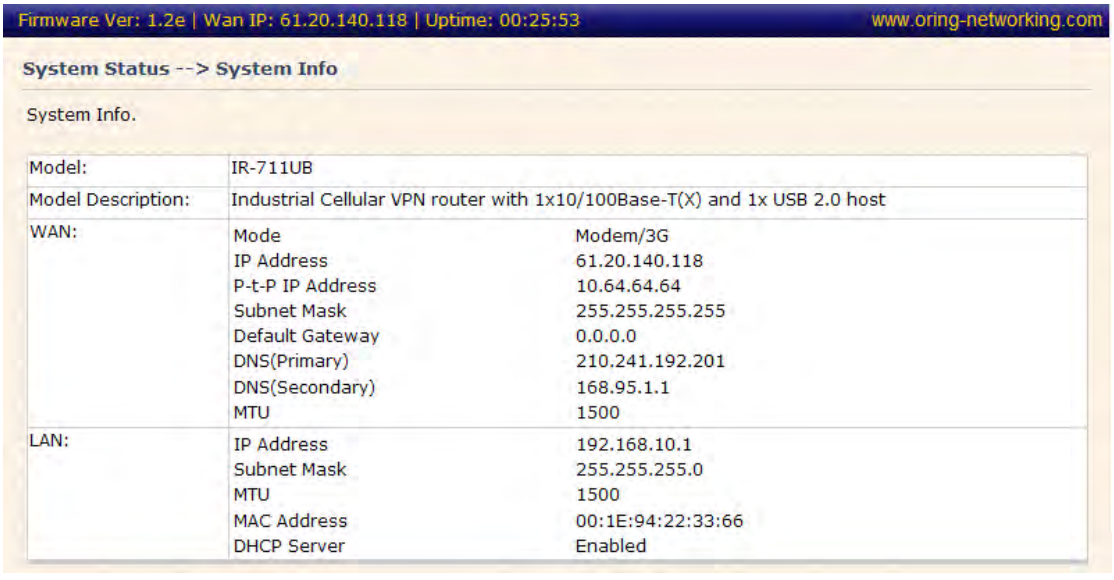
Login screen

Step 4: WAN connection

Click the **Basic Setting** in the top menu to enter the **WAN** configuration page, User can use **modem/3G** as WAN connection, please plug in your USB to RS232 converter with modem or 3G USB modem directly (HUAWEI E220 is supported).

Step 6: Review the router settings and check router status

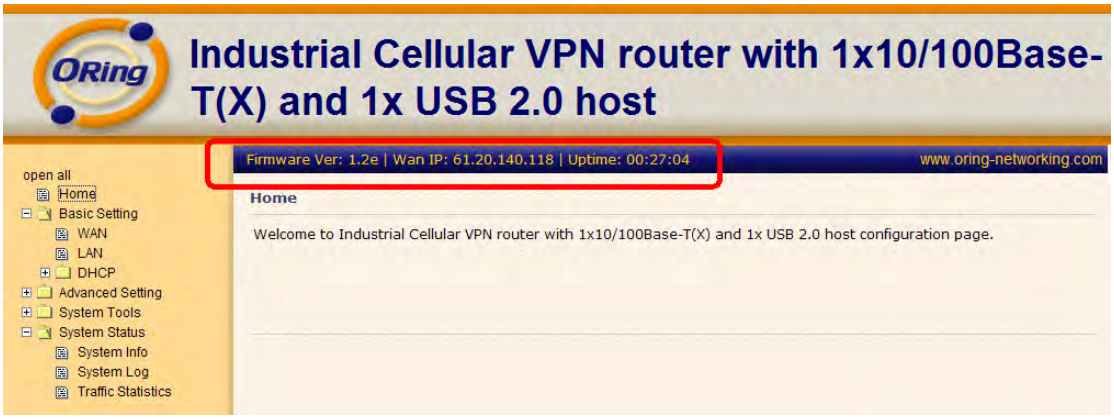
Click the **System Status** in the top of the menu, the system info page will be shown. You can check all the configuration and status of the router.



System status Screen

5.2 Main Interface

The **Home** screen will be shown when login successfully.



Main Interface

In the page, you can check the Firmware version, the router running time and the WAN IP setting.

The following table describes the labels in this screen.

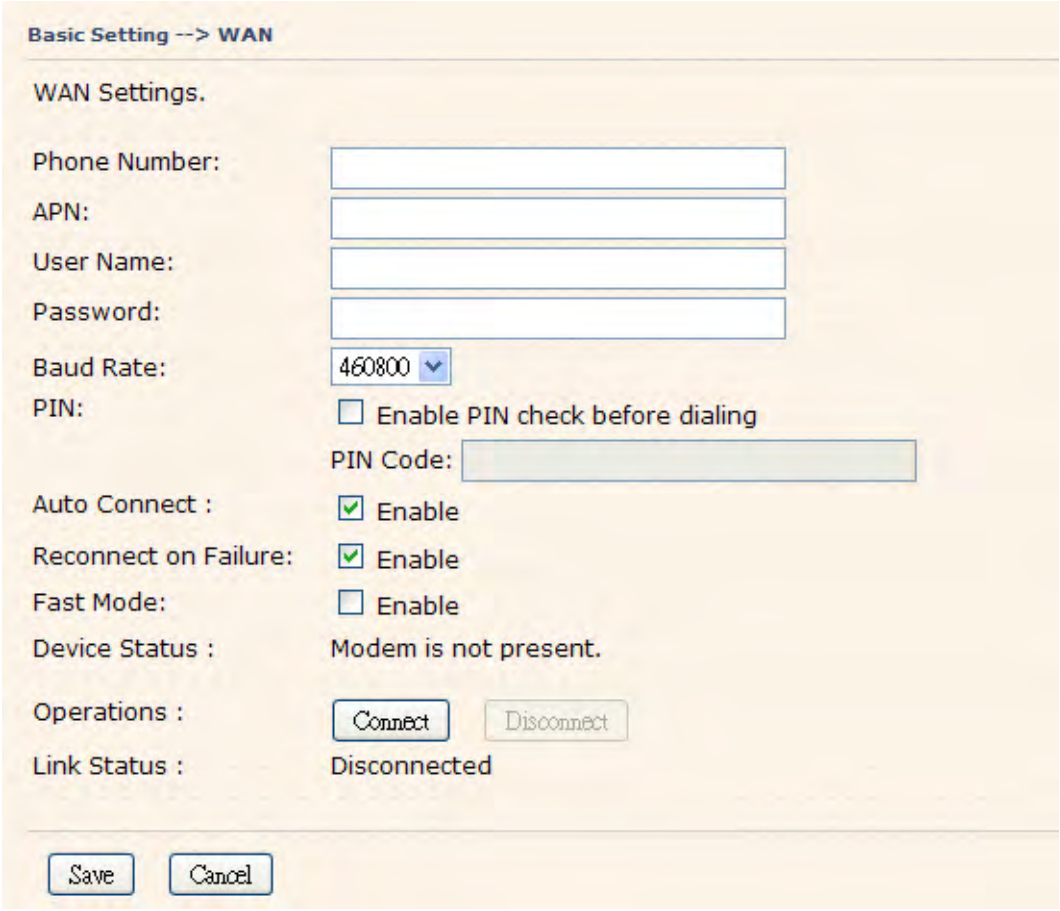
Label	Description
Firmware	Show the current firmware version.
Uptime	Show the elapsed time since the VPN router is started.
Wan IP	Show the WAN IP address.

5.3.1 Basic Setting

WAN

The IR-71UB VPN router provide 3G Modem WAN connection.

First you need an USB to RS232 converter and a modem or 3G USB modem (HUAWEI E220 is supported) directly. Please connect the converter or 3G modem to the USB port before starting the VPN router.



Modem/3G Screen

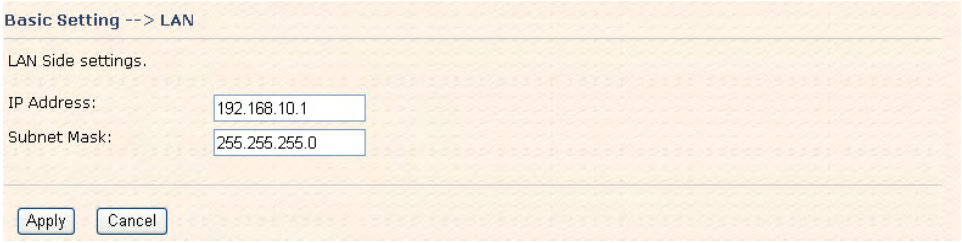
The following table describes the labels in this screen.

Label	Description
Phone Number	Telephone number provided by your ISP.
APN	Provide by your ISP
User Name	User name provided by your ISP.
Password	Password provided by your ISP.
PIN	Enter the PIN code if PIN check is required.
Auto Connect	If this option is enabled, the connection will be called up when router boots up.

Device Status	Show the status of Medem/3G device.
Operations	Click "**Connect**" to call up the Modem/3G. Click "**Disconnect**" to shut down the connection.
Link Status	Show the status of connection, **up**, **down** or **connecting**.

LAN

These are the IP settings of the LAN interface for the IR-711UB VPN router. The LAN IP address is privately for your internal network and can not be exposed on the Internet.



LAN Screen

The following table describes the labels in this screen.

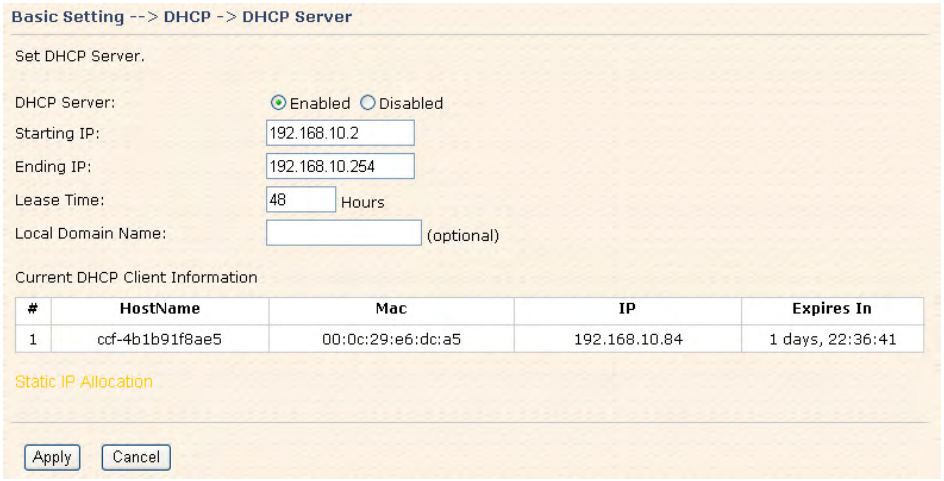
Label	Description
IP Address	The IP address of the LAN interface, the default IP address is 192.168.10.1
Subnet Mask	The Subnet Mask of the LAN interface, the default Subnet mask is 255.255.255.0

DHCP

DHCP stands for Dynamic Host Control Protocol. The IR-711UB VPN router has a built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

Set your computers to be DHCP clients by setting their TCP/IP settings to Obtain an IP Address Automatically. The DHCP server will allocate an unused IP address from the IP address pool to the requesting computer automatically.

1. DHCP Sever


Basic Setting --> DHCP -> DHCP Server
Set DHCP Server.
DHCP Server: Enabled Disabled
Starting IP: 192.168.10.2
Ending IP: 192.168.10.254
Lease Time: 48 Hours
Local Domain Name: (optional)
Current DHCP Client Information
HostName Mac IP Expires In
1 ccf-4b1b91f8ae5 00:0c:29:e6:dc:a5 192.168.10.84 1 days, 22:36:41
Static IP Allocation
Apply Cancel

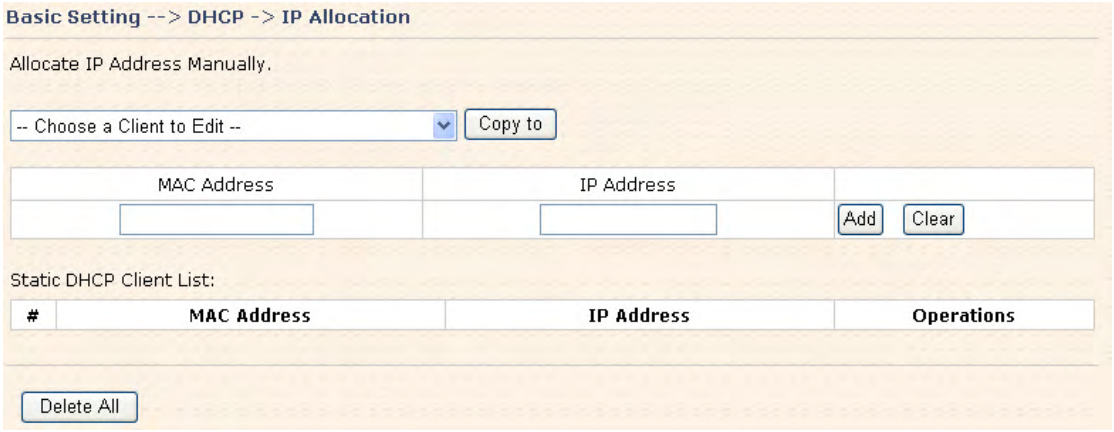
DHCP Server Screen

The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server. The default setting is Enable
Starting IP	The starting IP address of the IP range for the DHCP server
Ending IP	The ending IP address of the IP range for the DHCP server
Lease Time	The period of time for the IP to be leased. Enter the Lease time. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of private network. It is optional.
Current DHCP Client Information	List of the computers on your network that are assigned an IP address by internal DHCP server.

2. IP Allocation

The IP Allocation provides one-to-one mapping of MAC address to IP address. When a computer with the MAC address requesting an IP from the IR-711UB VPN router, it will be assigned with the IP address according to the mapping. You can choose one from the client lists and add it to the mapping relationship.



IP Allocation Screen

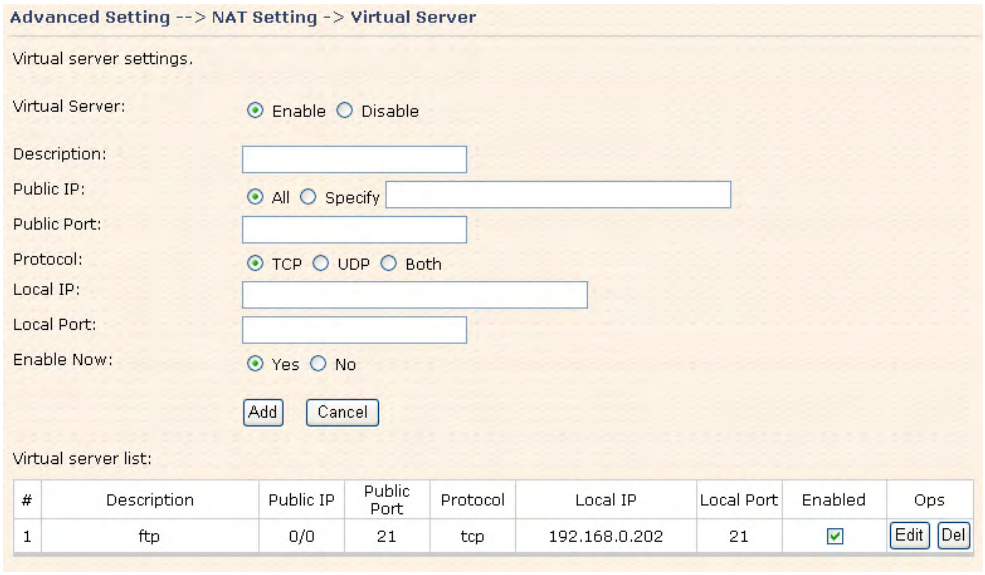
The following table describes the labels in this screen.

Label	Description
Choose a Client to Edit	The list shows the MAC addresses and IP addresses that are already assigned by IR-711UB. Choose one from the list and click **Copy to** button for editing.
MAC Address	The MAC addresses of the computer.
IP Address	The IP address to be related to the MAC address.
Static DHCP Client List	The list shows the MAC address and IP address one-to-one relationship.

NAT Setting

1. Virtual Server

Virtual Server is used for setting up public services on the LAN, such as DNS, FTP and Email. Virtual Server is defined as a Local Port to the LAN servers, and all requests from Internet to this Local port will be redirected to the computer specified by the Local IP. Any PC that was used for a virtual server must have static or reserved IP Address because its IP address may change when requesting IP by DHCP.


Advanced Setting --> NAT Setting -> Virtual Server
Virtual server settings.
Virtual Server: Enable Disable
Description:
Public IP: All Specify
Public Port:
Protocol: TCP UDP Both
Local IP:
Local Port:
Enable Now: Yes No
Add Cancel
Virtual server list:
Description Public IP Public Port Protocol Local IP Local Port Enabled Ops
1 ftp 0/0 21 tcp 192.168.0.202 21 Edit Del

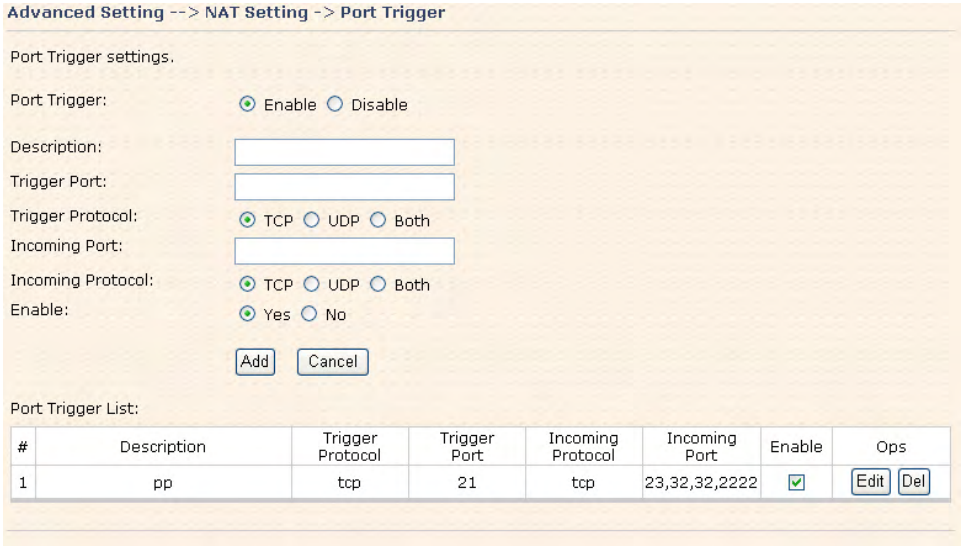
Virtual Server

The following table describes the labels in this screen.

Label	Description
Virtual Server	Enable or disable Virtual Server.
Description	Enter the description of the entry. Acceptable characters consist of '**0-9**', '**a-z**', '**A-Z**'. This field accepts null value.
Public IP	Enter the public IP that is allowed to access the virtual service, if not specified, choose All.
Public Port	The port number on the WAN (Wide Area Network) side that will be used to access the virtual service.
Protocol	The protocol used for the virtual service.
Local IP	The IP of the computer that will be providing the virtual service.
Local Port	The port number of the service used by the Private IP computer.
Enable Now	Enable the virtual server entry after adding it.
Virtual server list	Click **Edit** to edit the virtual service entry, **Del** to delete the entry.

2 Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Trigger is used for some of the applications that can work with an NAT router.


Advanced Setting --> NAT Setting -> Port Trigger
Port Trigger settings.
Port Trigger: Enable Disable
Description:
Trigger Port:
Trigger Protocol: TCP UDP Both
Incoming Port:
Incoming Protocol: TCP UDP Both
Enable: Yes No
Add Cancel
Port Trigger List:
Description Trigger Protocol Trigger Port Incoming Protocol Incoming Port Enable Ops
1 pp tcp 21 tcp 23,32,32,2222 Edit Del

Port Trigger Screen

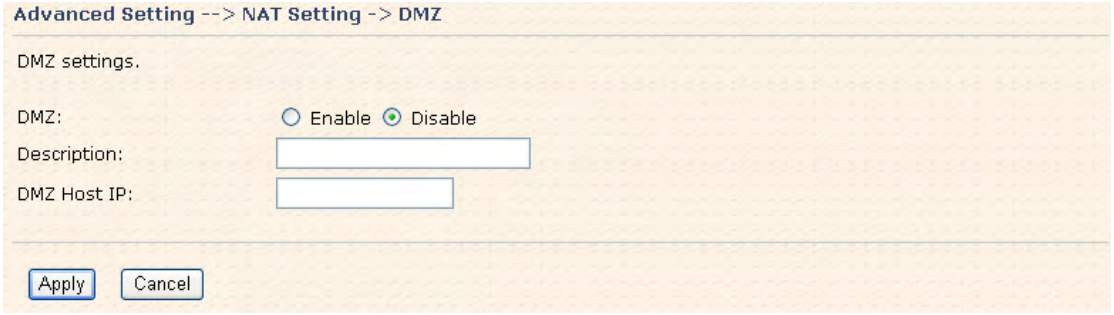
The following table describes the labels in this screen.

Label	Description
Port Trigger	Enable or disable Port Trigger.
Description	This is the description for the entry.
Trigger Port	This is the port used to trigger the application.
Trigger Protocol	This is the protocol used to trigger the application.
Incoming Port	This is the port number on the WAN side that will be used to access the application.
Enable	Enable the rule after adding the entry.
Port Trigger List	Click **Edit** to edit the entry, click **Del** to delete the entry.

3. DMZ

It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes.

Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ may expose your local network with variety of security risks, so only use this option carefully.



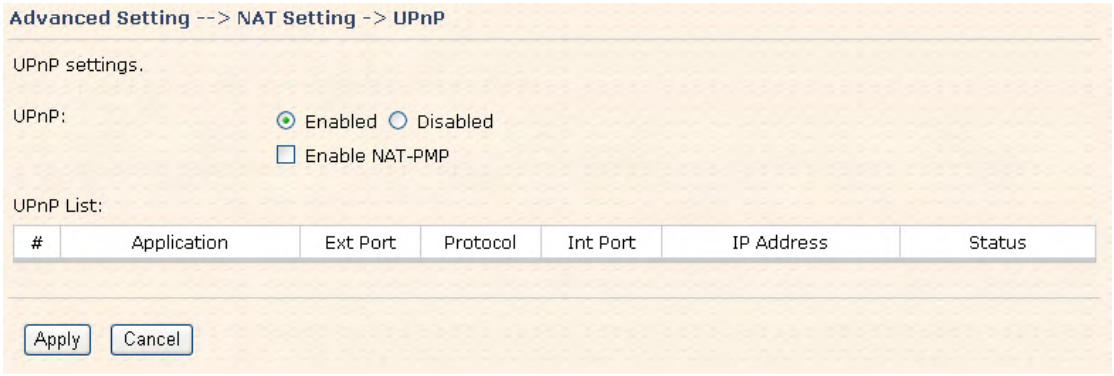
DMZ Screen

The following table describes the labels in this screen.

Label	Description
DMZ	Enable or disable the DMZ.
Description	Description for the DMZ host entry.
DMZ Host IP	Enter the IP address of the computer to be in the DMZ.

4. UPnP

The UPnP (Universal Plug and Play) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



UPnP Screen

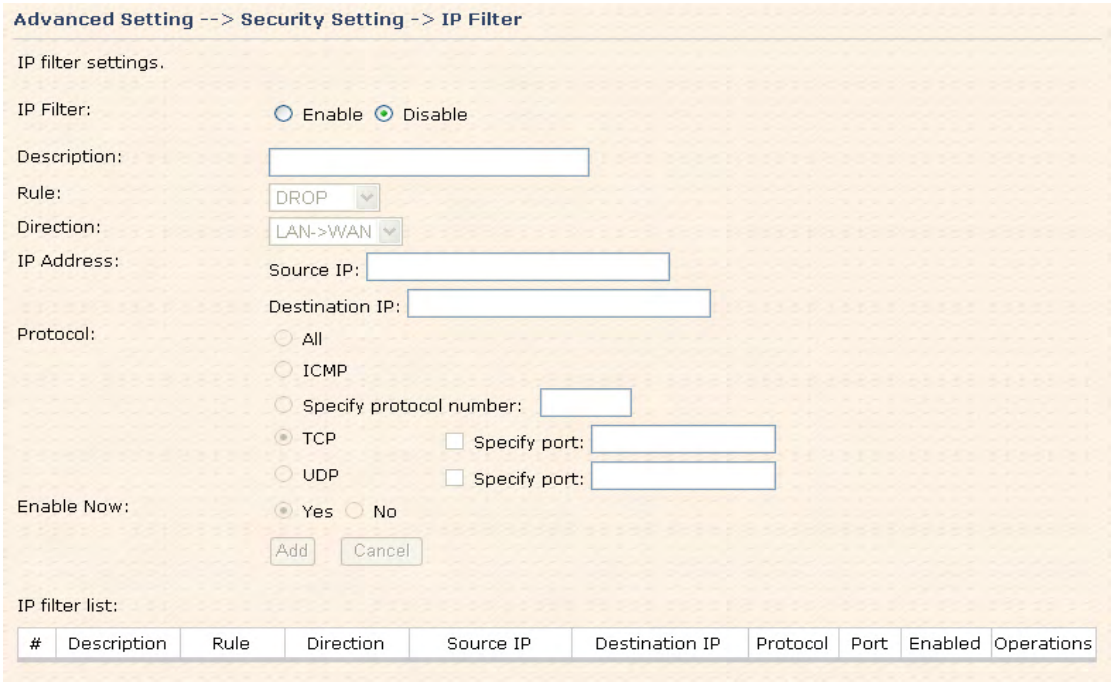
The following table describes the labels in this screen.

Label	Description
UPnP	Enable or disable UPnP.
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact with each other. NAT-PMP operates with UDP. It essentially automates the process of port forwarding. Check the box to enable NAT-PMP.
UPnP List	This table lists the current auto port forwarding information. **Application:** The application that generates this port forwarding. **Ext Port:** The port opened on WAN side. **Protocol:** The protocol type. **Int Port:** The port redirected to the local computer. **IP Address:** The IP address of local computer to be redirected to. **Status:** This status shows if the entry is valid or not.

Security Setting

1. IP Filter

Filters are used to deny or allow LAN computers from accessing the internet. It also allows or denies WAN hosts to access LAN computers.



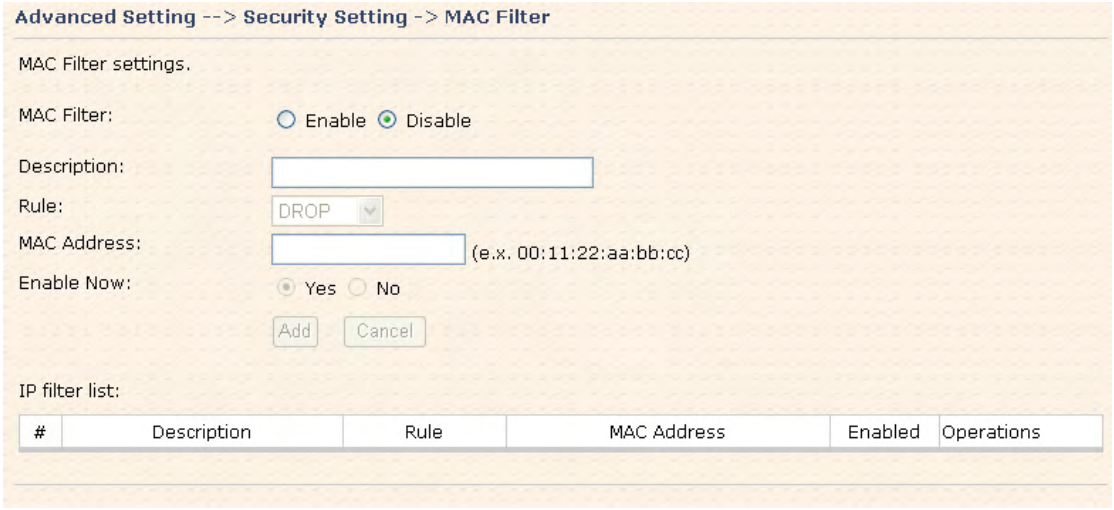
IP Filter Screen

The following table describes the labels in this screen.

Label	Description
IP Filter	Enable or disable the IP Filter.
Description	Enter description for the entry.
Rule	Select **DROP**, **ACCEPT** and **REJECT** rule for the entry.
Direction	Specify the direction of the data flow that is to be filtered.
IP Address	Enter the IP address of the source and destination computer.
Protocol	Choose which protocol to be filtered.
Enable Now	Enable the entry after adding it.
IP filter list	Click **edit** for editing the entry, click **Del** to delete the entry.

2. MAC Filter

Filters are used to deny or allow LAN computers from accessing the internet, according to their MAC address.



MAC Filter Screen

The following table describes the labels in this screen.

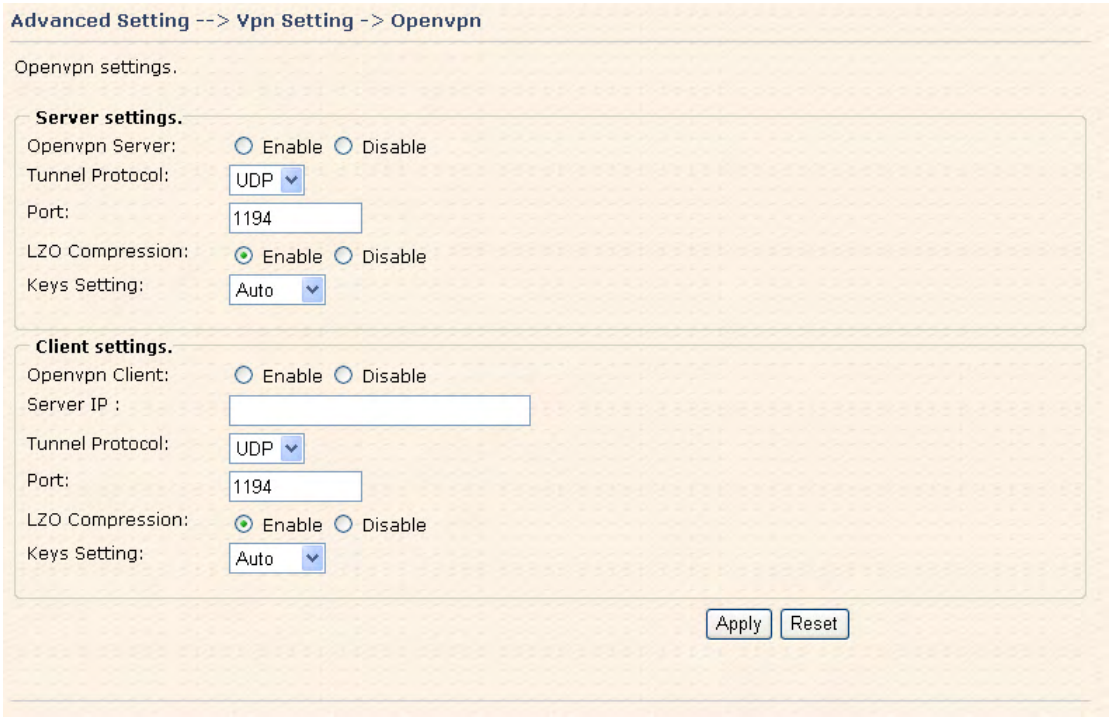
Label	Description
MAC Filter	Enable or disable the MAC Filter.
Description	Enter the description for the entry.
Rule	Select **DROP**, **ACCEPT** and **REJECT** rule for the entry.
MAC Address	Enter the MAC address to be filtered.
Enable Now	Enable the entry after adding it.
IP filter list	Click **Edit** for editing the entry, click **Del** to delete the entry.

VPN Setting

VPN Setting is settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin, authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

1. Open VPN

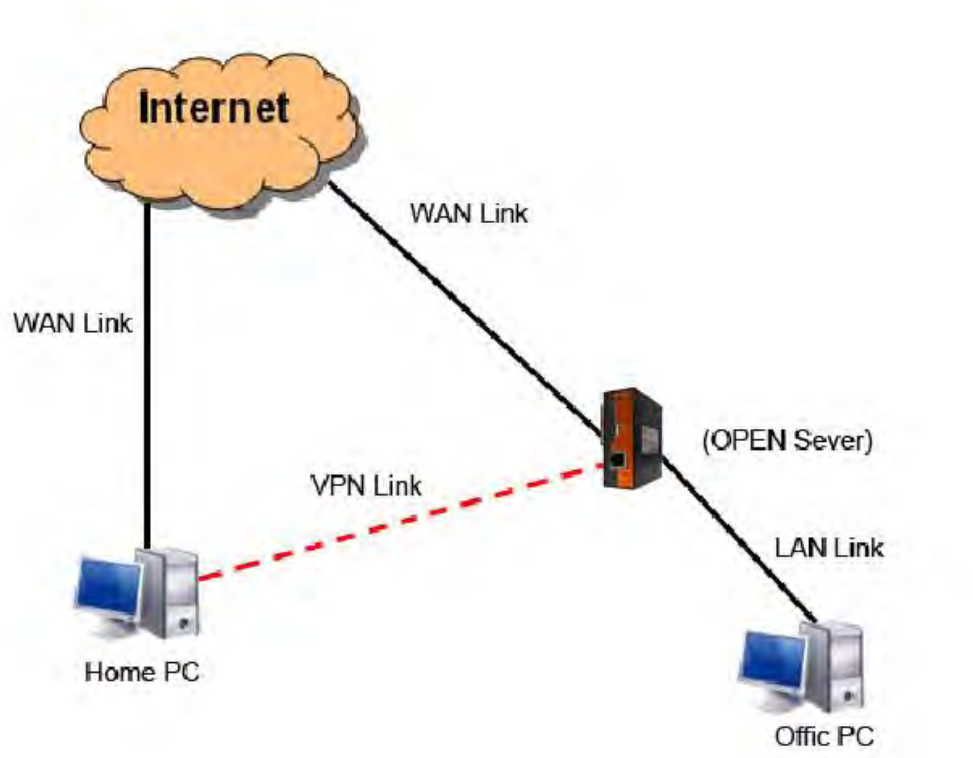
Open VPN is a full-functioned SSL VPN solution which can accommodates a wide range of configurations including remote access, site-to-site VPNs, , and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls.



Open VPN Screen

The following topology shows the common use of VPN connection from WAN side.

1: Open VPN Server



Connection to Open VPN Server

Before connecting to the Openvpn server of IR-711UB VPN router, please install openvpn client software for your windows PC. It can be downloading from http://openvpn.net/download.html#stablel. The current version of Openvpn used in IR-711UB is version 2.0.9. The corresponding software for client should be installed. The following table describes the labels in this screen.

Label	Description
Open VPN Server	Enable or disable the function of Open VPN Server.
Tunnel Protocol	Select UDP or TCP protocol.
Port	Input the number about the port, and the default is 1194.
LZO Compression	Enable or disable the function of LZO Compression.
Keys Setting	Select Auto to use the preset certificates, select Manual to paste your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website.

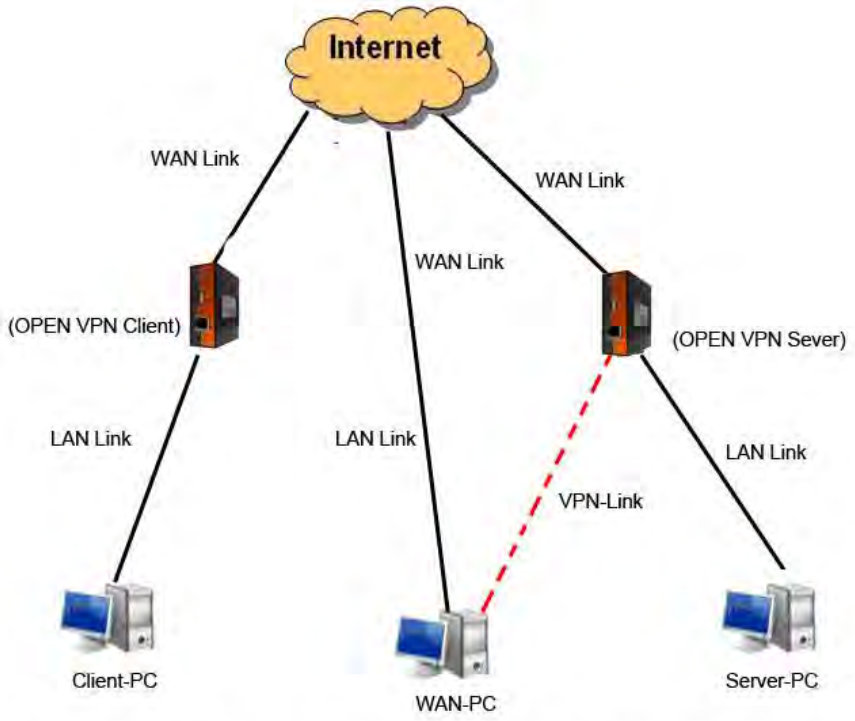
2: Open VPN Client

Two routers are needed for creating site-to-site VPN connection using this mode.

The following table describes the labels in this screen.

Label	Description
Open VPN Client	Enable or disable the function of Open VPN Client. You can allow or deny the Open VPN Client with this option.
Server IP	Enter the Open VPN Server IP address.
Tunnel Protocol	Select UDP or TCP protocol.
Port	Enter the port number, default is 1194.
LZO Compression	Enable or disable the LZO Compression.
Keys Setting	Select **Auto** to use the preset certificates, select **Manual** to paste your certificates. Please install software for openvpn client to generate your certificates and paste them here. For more information, please visit openvpn website.

3: Open VPN Server VS Client



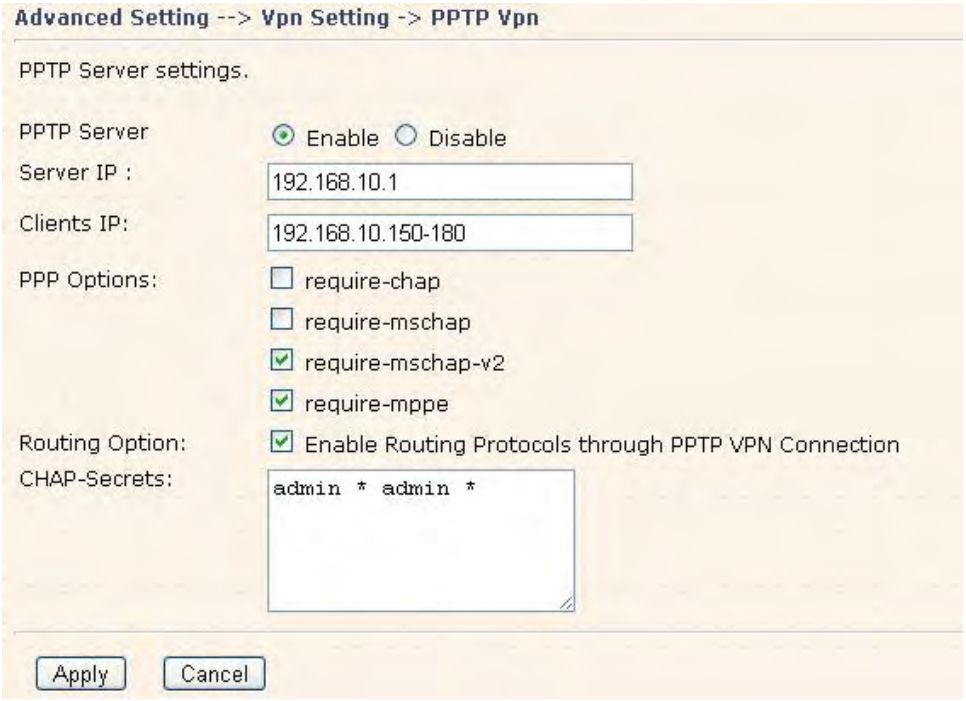
Client-PC and connect to Server-PC,WAN-PC

The chart above displays the connection of Open VPN Server and Client. The Server IP and Client IP address should configure with the same network domain.

2. PPTP VPN

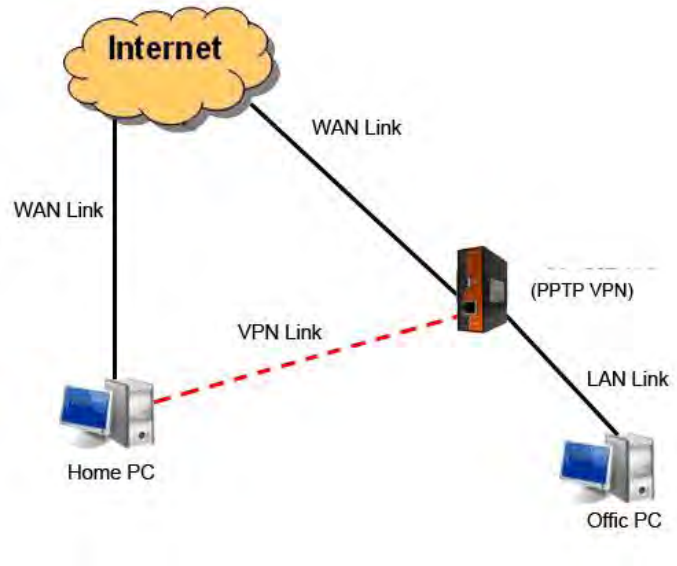
The PPTP (Point to Point Tunneling Protocol) VPN feature allows PC connected to the router from WAN port, just like connecting in the LAN.

To create a PPTP connection to the router, you should create a PPTP network connection if you are using a window PC. The steps are: **Right click Network > property > create a new connection > connect to my work space (VPN) > use VPN to internet > enter the user name and password** which are set in the page.



PPTP VPN Screen

The following topology shows the common use of PPTP connection from the internet.



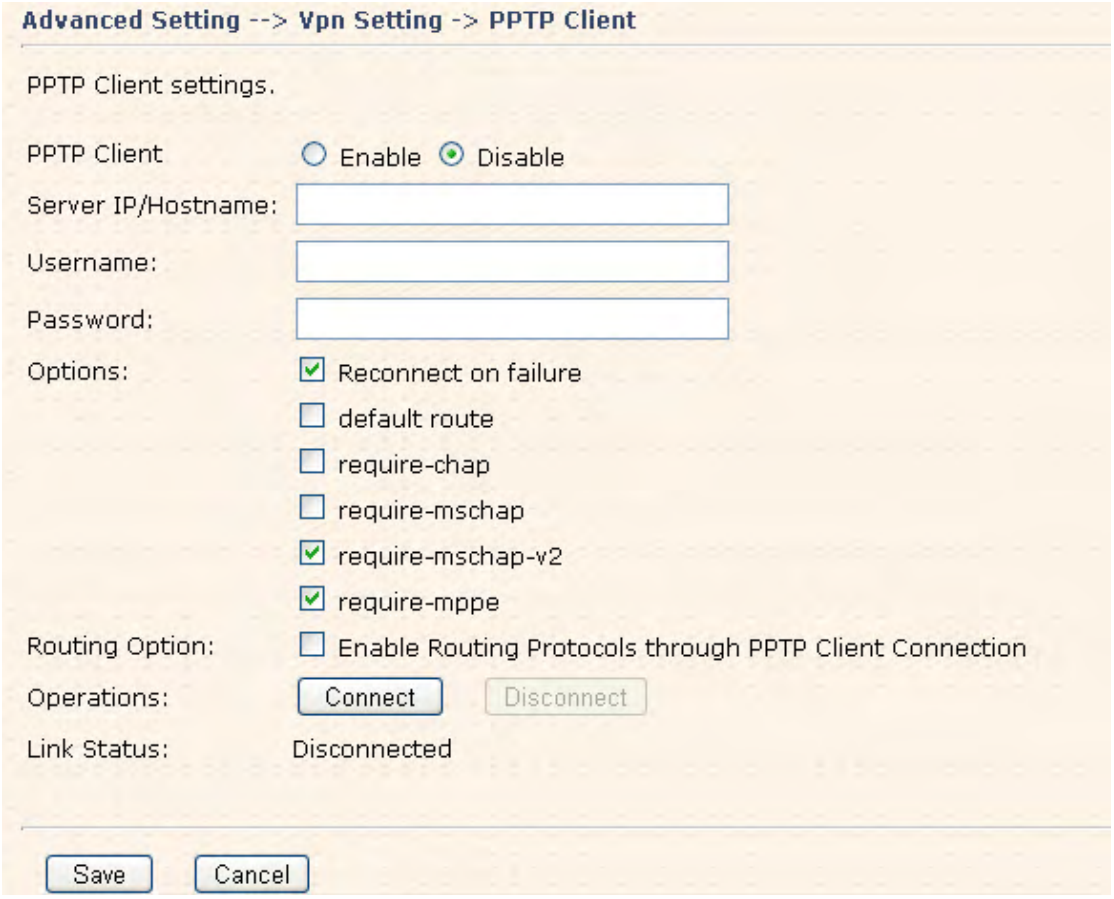
Connection to PPTP VPN Server

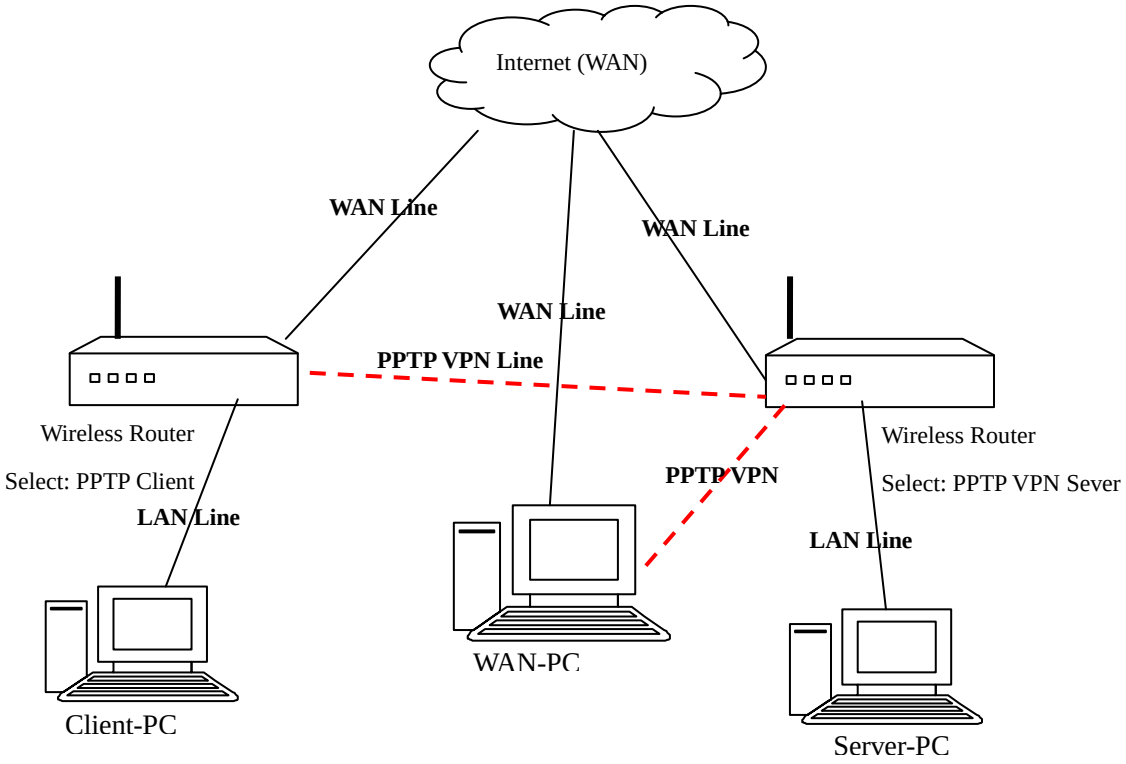
The following table describes the labels in this screen.

Label	Description
PPTP Server	Enable or disable PPTP VPN Server.
Server IP	Enter the server side IP address, default is the LAN port IP.
Client IP	Enter the IP address range, format is as **192.168.10.xx-xx**, connected client will be assigned the IP address.
PPP Options	Users can select the following Encryption Protocol(Need to be the same as client) 1、Challenge Handshake Authentication Protocol (CHAP) 2、Microsoft PPP Challenge Handshake Authentication Protocol(MSCHAP) 3、Microsoft PPP Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) 4、Microsoft Point-To-Point Encryption (MPPE) Protocol Detail that encrypt each, please consult http://technet.microsoft.com/zh-tw/library/cc757631(WS.10).aspx
Routing Option	User can select check box, enable or disable Routing Protocols through PPTP VPN Connection
CHAP-Secrets	Enter the username and password pairs, format is as **user * pass ***, multiple username password pairs are allowed.

3. PPTP Client

If the router A want to link with the others which is not in the same network with the router A, the function of PPTP client should support in the router page.





Result: Client-PC can connect to Server-PC, WAN-PC.

Label	Description
PPTP Client	Enable or disable PPTP Client.
Server IP/Hostname	Enter the server IP address or hostname.
Username/Password	Enter the username and password which is signed by PPTP server.
Option	Reconnect on failure: Pitch on this option, it will be reconnect when the link is on failure. Users can select the following Encryption Protocol(Need to be the same as Server) 1、 Challenge Handshake Authentication Protocol (CHAP) 2、 Microsoft PPP Challenge Handshake Authentication Protocol(MSCHAP) 3、 Microsoft PPP Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) 4、 Microsoft Point-To-Point Encryption (MPPE) Protocol Detail that encrypt each, please consult http://technet.microsoft.com/zh-tw/library/cc757631(WS.10).aspx

Operations	Click "Connect" to link the server, if or not, you can click ""Disconnect" to break off from the server.
Link Status	Show the status about the link.

Routing Protocol (Routing Setting)

This page shows the information of routing table. The initial state of the router connect to the WAN, it will be based on the outside networks to access the routing table automatically. You can refer the shows about the bellow page.

Current Routing Table:

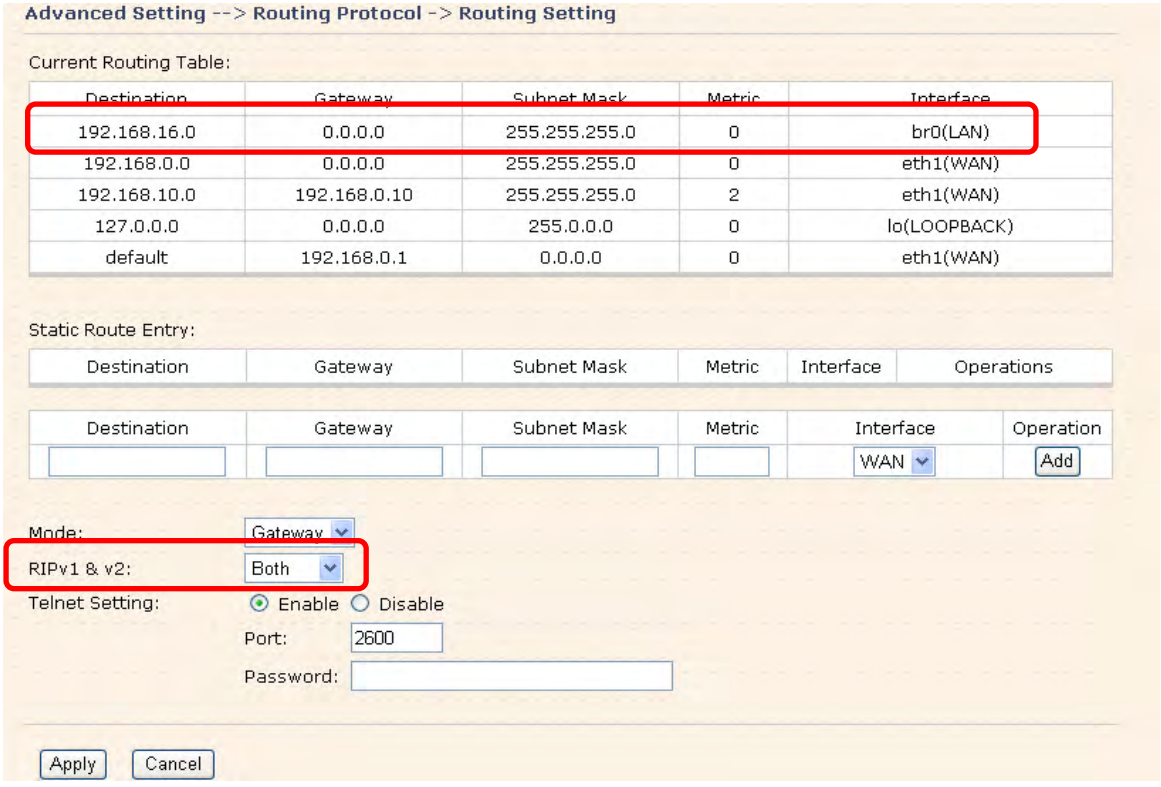
Destination	Gateway	Subnet Mask	Metric	Interface
192.168.16.0	0.0.0.0	255.255.255.0	0	br0(LAN)
192.168.0.0	0.0.0.0	255.255.255.0	0	eth1(WAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)
default	192.168.0.1	0.0.0.0	0	eth1(WAN)

The table shows the normal routing table

1. Use Dynamic Routing

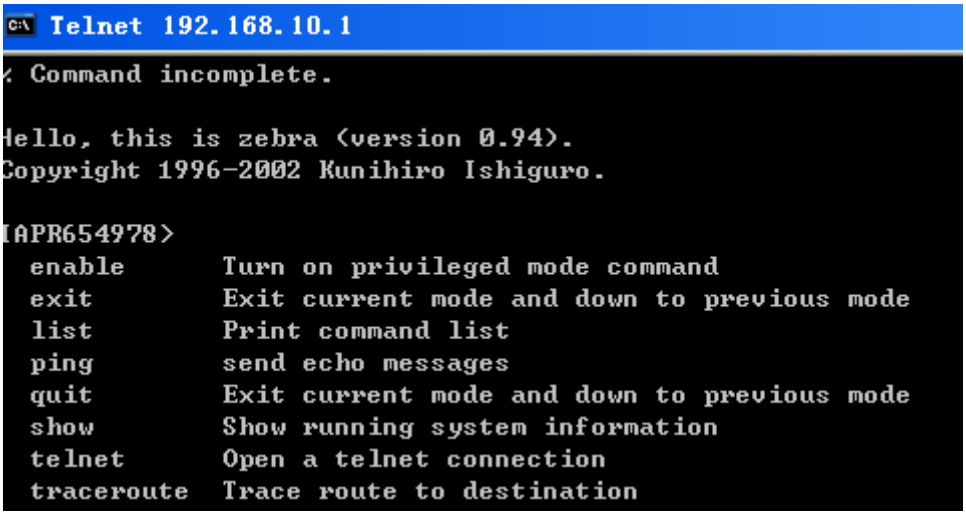
Use the dynamic routing, you should not choose "Disable" about the **RIPv1 & v2** in the routers.

Click "Apply", and you can see the more information in the **Current Routing Table**, which shows the network segment of the other router.



Label	Description
Current Routing Table	Show the current the routing information.
Static Router Entry	Not RIP and enter the right value in the textbox will be showing.
Mode	If you want to the PC in the router can visit the outside network, only choose the **Gateway Mode**; if or not, you choose the **Router Mode.**
RIPv1 &v2	Choose "Disable" in the Static routing.
Telnet Setting	Only use in the Dynamic routing.

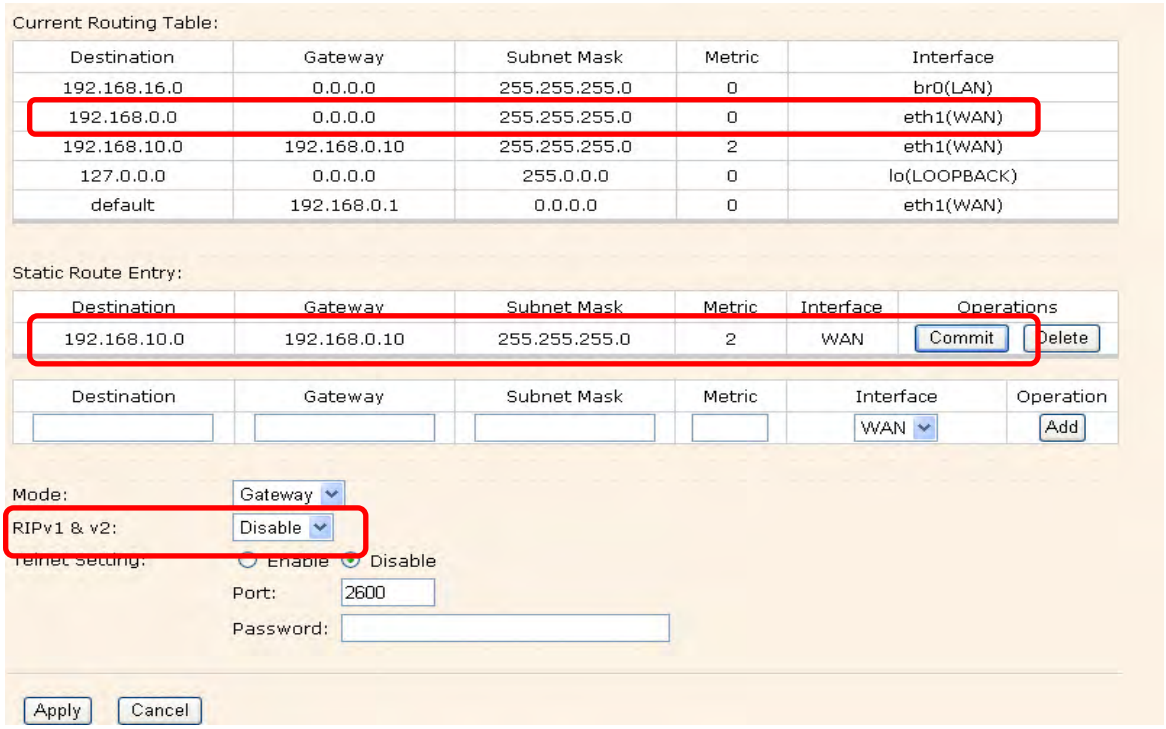
Simultaneously, only use the Telnet function in the dynamic routing. You can telnet the LAN IP and there are many orders.


Telnet 192.168.10.1
% Command incomplete.
Hello, this is zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.
IAPR654978>
enable Turn on privileged mode command
exit Exit current mode and down to previous mode
list Print command list
ping send echo messages
quit Exit current mode and down to previous mode
show Show running system information
telnet Open a telnet connection
traceroute Trace route to destination

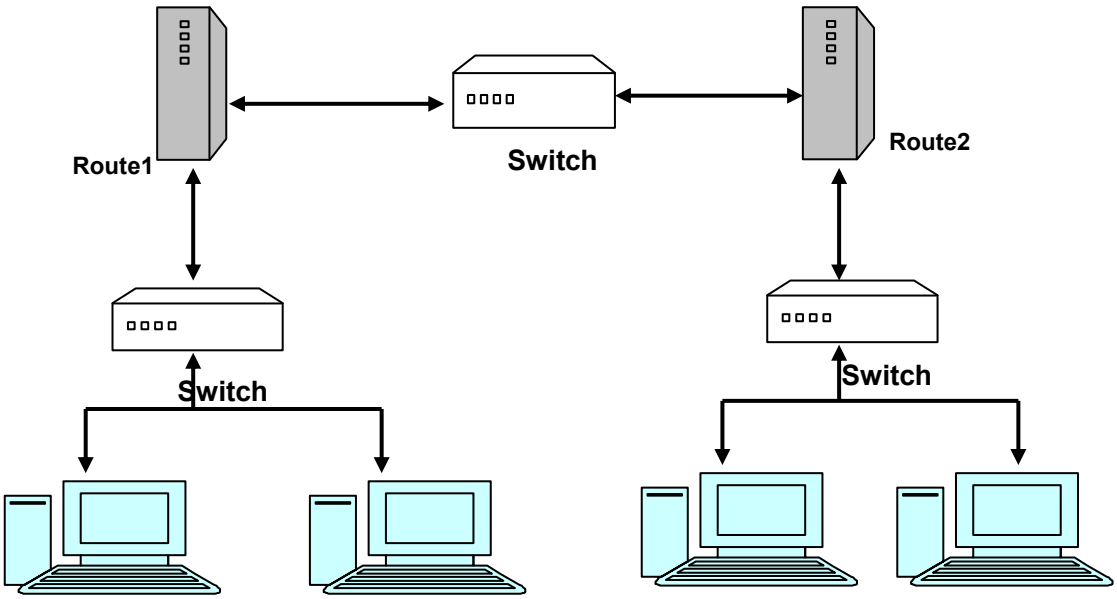
2. Use Static Routing

Use the Static routing, you should choose "Disable" about the **RIPv1 & v2** in the routers.

Click "Apply", and you can see the more information in the **Current Routing Table** and **Static Route Entry**, which shows the network segment of the other router.


Current Routing Table:
Destination Gateway Subnet Mask Metric Interface
192.168.16.0 0.0.0.0 255.255.255.0 0 br0(LAN)
192.168.0.0 0.0.0.0 255.255.255.0 0 eth1(WAN)
192.168.10.0 192.168.0.10 255.255.255.0 2 eth1(WAN)
127.0.0.0 0.0.0.0 255.0.0.0 0 lo(LOOPBACK)
default 192.168.0.1 0.0.0.0 0 eth1(WAN)
Static Route Entry:
Destination Gateway Subnet Mask Metric Interface Operations
192.168.10.0 192.168.0.10 255.255.255.0 2 WAN Commit Delete
Destination Gateway Subnet Mask Metric Interface Operation
WAN Add
Mode: Gateway
RIPv1 & v2: Disable
Telnet Setting: Enable Disable
Port: 2600
Password:
Apply Cancel

Use the dynamic routing; it will have many ways such as RIP, OSPF.BGP. In this router, we use the RIP Protocol to finish the dynamic routing table.



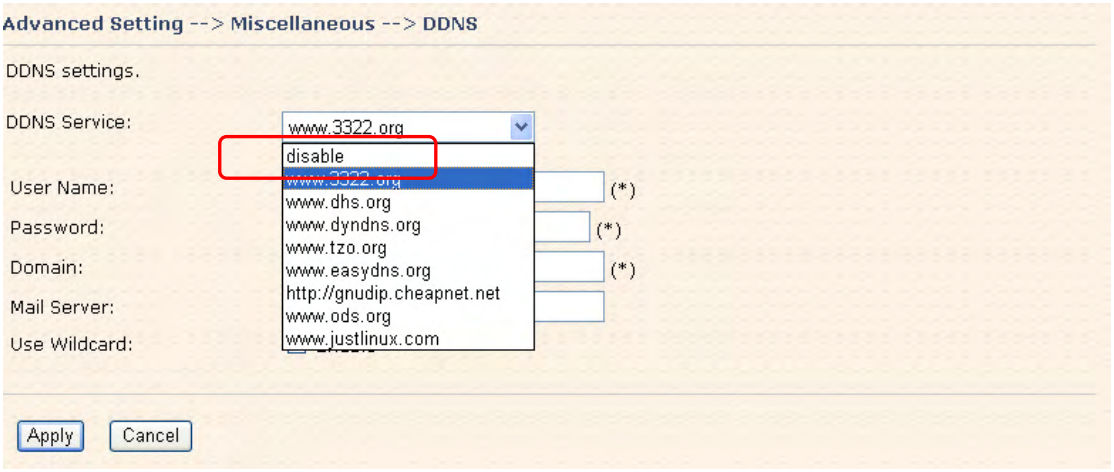
The Routing Topography

RIP, Routing Information Protocol, is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm.

After all settings, PC1 can visit PC2 which is different network segment of the PC1.

Miscellaneous (DDNS)

Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP address.



DDNS Screen

For example, Choose DDNS Service: www.3322.org and configure the following instructions:

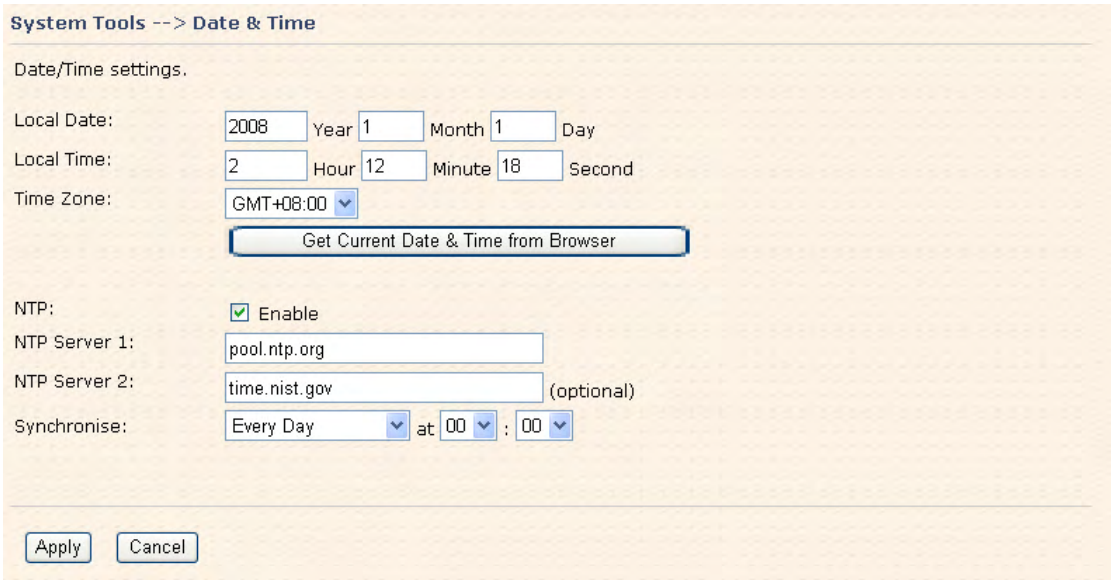
The following table describes the labels in this screen.

Label	Description
User Name	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.
Domain	Enter the domain names provided by your dynamic DNS service provider.
Mail Server	Enter the mail server if provided.
Use Wildcard	Check the box the enable wildcard option.

5.3.2 System Tools

Date & Time

In this page, you can set the date & time of the device. The correct date & time will be helpful for logging of system events. A NTP (Network Time Protocol) client can be used to synchronize date & time with NTP server through internet.



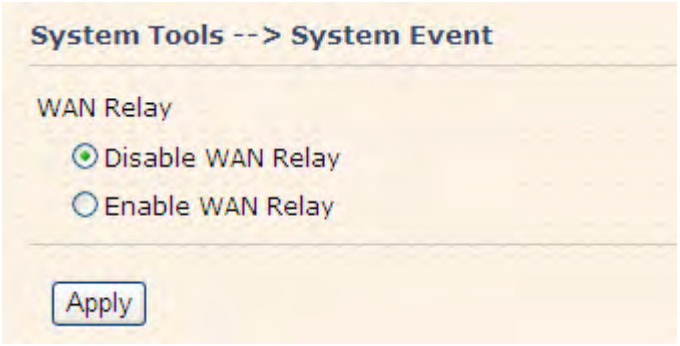
Date & Time Screen

The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date & Time from Browser	Click this button; you can set the time from your browser.
NTP	Enable or disable NTP function to synchronize time from the NTP server.
NTP Server 1	The primary NTP Server.
NTP Server 2	The secondary NTP Server.
Synchronize	This is the scheduled time when the NTP synchronization performed.

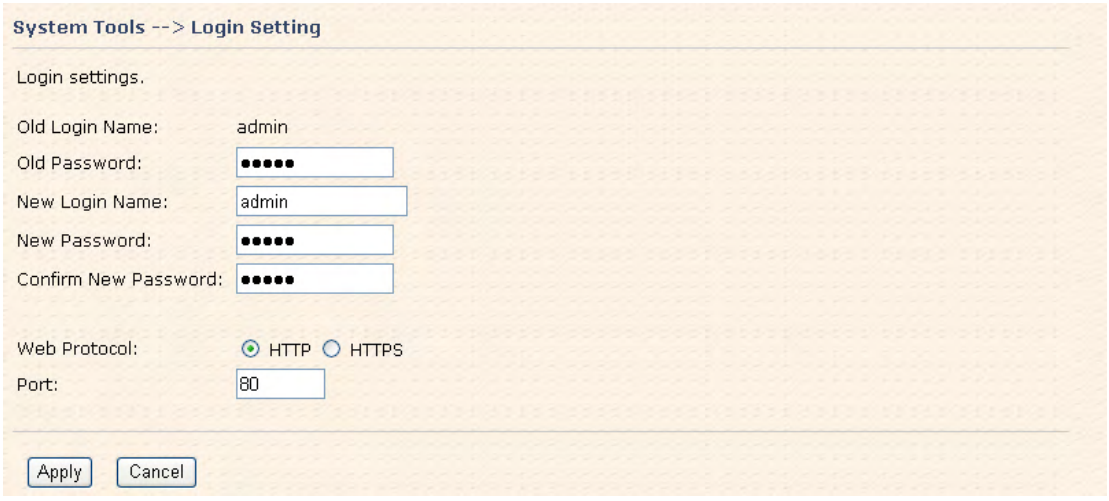
System Event

At this page, the administrator can select Enable or Disable WAN Relay.



Login Setting

At this page, the administrator can change the login name and password. The default name and password is **admin** and **admin**.



Login Setting Screen

The following table describes the labels in this screen.

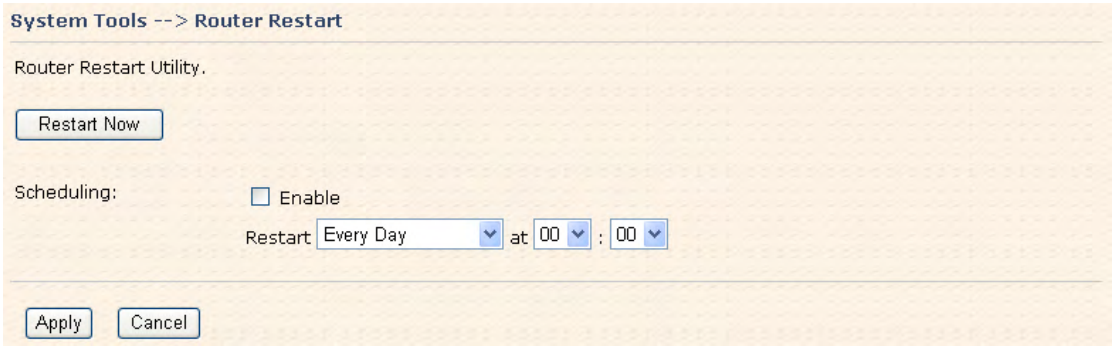
Label	Description
Old Name	This field shows the old login name.
Old Password	Before making a new setting, you should provide the old password for verification. Acceptable characters of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length. An empty password is also acceptable.

New Name	Enter a new login name. Acceptable characters of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 1 to 15 characters in length. An empty name is not acceptable.
New Password	Enter a new login password. Acceptable characters of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length.
Confirm New Password	Retype the password to confirm it. Acceptable inputs of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length.
Web Protocol	Choose the web management page protocol. HTTP and HTTPS are both supported.
Port	Choose the web management page port number. For HTTP, default port is 80; For HTTPS, default port is 443.

HTTPS (HTTP over SSL) is a Web protocol which encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

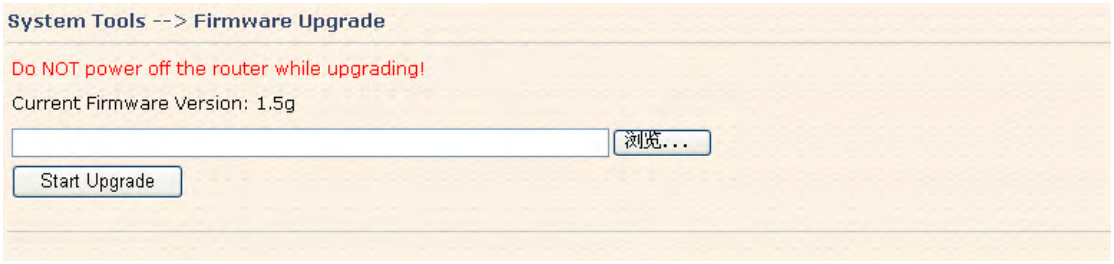
Router Restart

If you want restart the router through the **Warm Reset**, click **Restart Now** to restart the Wireless Router. Also, you can set a **Scheduling** time to make the router restart.



Router Restart Screen

Firmware Upgrade

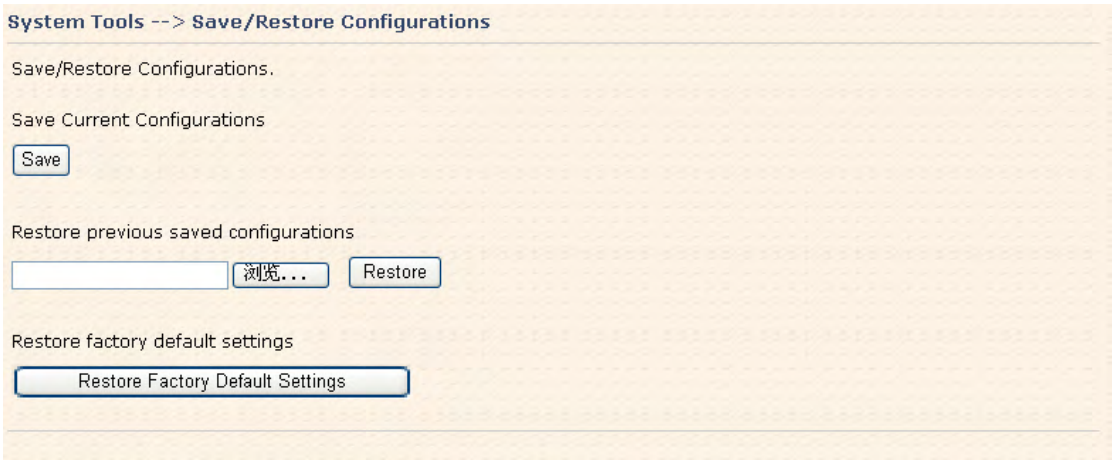

System Tools --> Firmware Upgrade
Do NOT power off the router while upgrading!
Current Firmware Version: 1.5g
浏览...
Start Upgrade

Firmware Upgrade Screen

Newer firmware may provide better performance or function extensions. To upgrade the new firmware, you need a firmware file which matches the model of this VPN router. It will take several minutes to upload and update the firmware. After the upgrade is done successfully, reboot the router to utilized new firmware.

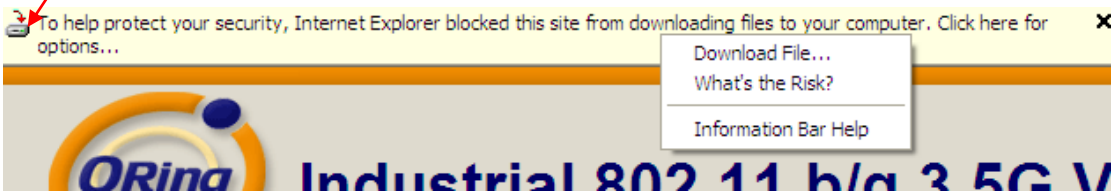
Important Notice: DO NOT POWER OFF THE ROUTER OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Save/Restore Configurations



Save/Restore Configurations Screen

Save: The configuration file can be downloaded. (Internet Explorer user will need to click on the protection bar on top and click choose "download files")

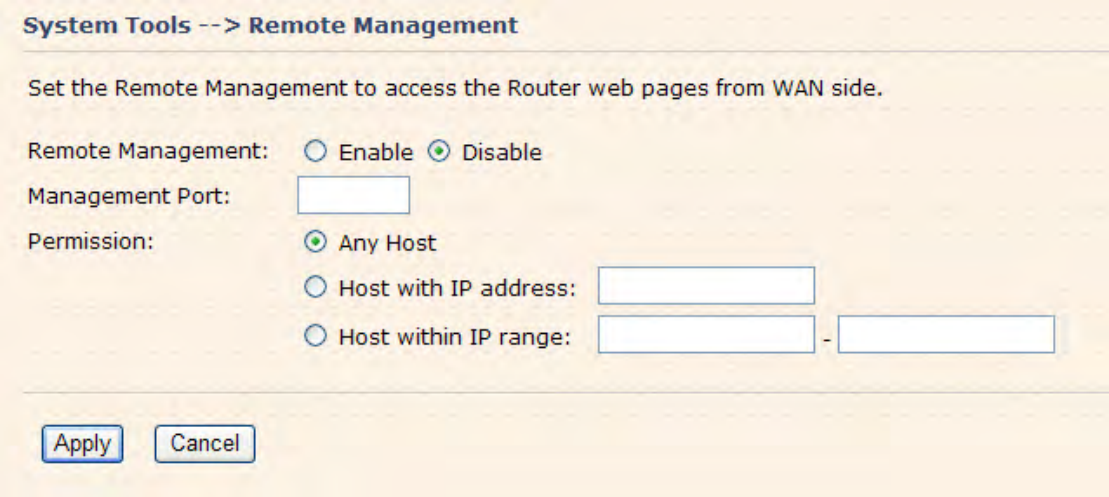

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...
Download File...
What's the Risk?
Information Bar Help

The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file into your PC.
Upload configuration	The configuration can be restored to the router. To reload a system settings file, click on **Browse** to browse your local hard drive and locate the system settings file previously saved. Click **Upload** when you have selected the file.
Restore Default Settings	You may also reset the router to the factory settings by clicking on **Restore Default Settings**. The router will reboot to validate the default settings.

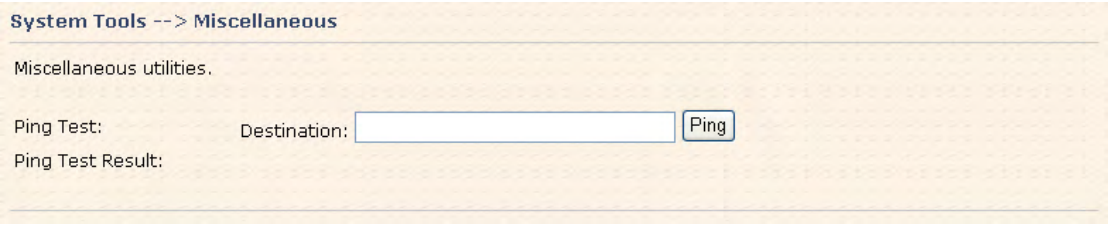
Remote Management

Remote Management function, open the Remote Management, that would allow the user via the Internet (WAN Port) Remote Management IR-711UB



Label	Description
Remote Management	Enable or Disable Remote Management.
Management Port	Input want to open port.
Permission	Users can define their own, allowing remote connection IP Location

Miscellaneous (Ping)

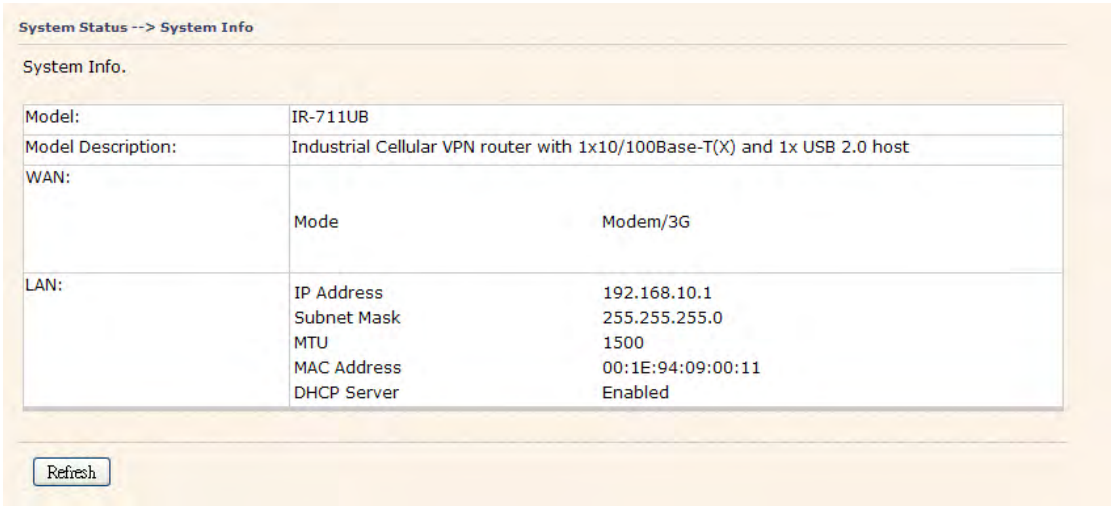


Miscellaneous Screen

The Ping Test is used to send Ping packets to test if a computer whether it is on the Internet or test if the WAN connection is OK. Enter a domain or IP in the destination box and click Ping to test.

5.3.3 System Status

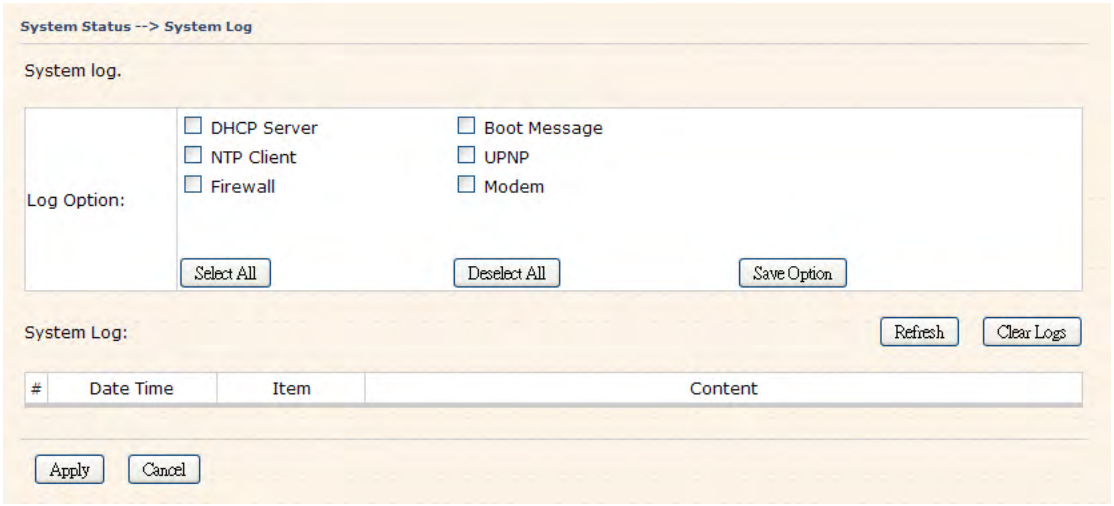
System Info



System Info Screen

This page displays the details information for the VPN router including model name, model description, firmware version, WAN and LAN settings.

System Log



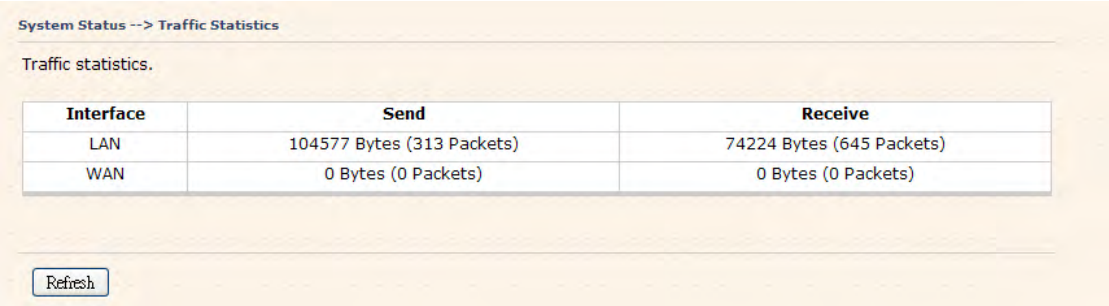
System Log Screen

The router keeps a running log of events and activities occurring on the router, several filters are provided for displaying related log entries.

Click the button '**Refresh**' to refresh the page.

Click the button '**Clear Logs**' to clear the log entries.

Traffic Statistics



Traffic Statistics Screen

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections.

Technical Specifications

LAN Interface	
RJ45 Ports	1 x 10/100Base-T(X), Auto MDI/MDI-X
Protection	Built-in 1.5KV magnetic isolation
Protocols	IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, HTTPS, SNMP
LED Indicators	(1.) PWR Ready: Green ON: Power is on and functioning normally. (2.) Status LED: Green ON: transmission data (3.) ETH Link / ACT: Orange ON/OFF: 100/10 Mbps Ethernet Green ON/Blinking: Ethernet active (4.) USB Modem LED: Green ON: USB modem is present Green Blinking: USB modem is transmitting data (5.) Fault: WAN link down (Red)
Power Requirements	
Power Input Voltage	PWR: 12 ~ 48VDC in 4-pin Terminal Block
Reverse Polarity Protection	Present
Power Consumption	3.3 Watts (USB device not included)
Fault Contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Environmental	
Operating Temperature	-20 to 70°C
Storage Temperature	-40 to 85°C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	26.1(W)x70(D)x95(H) mm
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPR (EN55022) Class A

EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Safety	IEC 60950-1
Waranty	5 years

Appendix A

How to configure openvpn and use openvpn in the Windows?

Step 1: Download openvpn-gui-1.0.3.exe and run the install program. If there is a pop-up box opened at the course of the install, please you click "Continue…" and finish the install. Default path is: "C:\Program Files\OpenVPN".

Step 2: Configure the OpenVPN Server.

(1) Modify the parts in "C:\Program Files\OpenVPN\easy-rsa\vars.bat.sample" as follows:

set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=Oring
set KEY_EMAIL=staff@oring-networking.com

(2) Start > Run… > Input "cmd", and enter into Command Prompt. > Input "cd c:\Program Files\openvpn\easy-rsa"

*Run **init-config.bat**: create the vars.bat and openssl*
*Run **vars.bat, clean-all.bat**: create new empty index and serial files*
*Run **build-ca.bat**: build a CA key*
*Run **build-dh.bat**: build a DH file for server side*
*Run **build-key-server.bat server**: build a private key/certificate for openvpn server*

*Run **build-key.bat client**: build key files in PEM format for client machine*

All inborn secret-keys are in "c:\Program Files\openvpn\easy-rsa\keys".

OpenVPN Server needs files: **ca.crt, dh1024.pem, server.crt, server.key,** and copy to "C:\Program Files\OPENVPN\Config".

OpenVPN Client needs files: **ca.crt, client.crt, client.key**, and copy to "C:\Program Files\OPENVPN\Config".

(3) Edit the server.ovpn in the openvpn server and client.ovpn in the openvpn client.

server.ovpn:

Modify according to by the router web settings

```
# Tunnel options
        mode server         # Set OpenVPN major mode
        proto udp           # Setup the protocol (server)
        port 1194           # TCP/UDP port number
        dev tap0            # TUN/TAP virtual network device
        keepalive 15 60     # Simplify the expression of --ping
        #daemon                 # Become a daemon after all initialization
        verb 3              # Set output verbosity to n
        comp-lzo            # Use fast LZO compression

        # OpenVPN server mode options
        client-to-client    # tells OpenVPN to internally route client-to-client traffic
        duplicate-cn        # Allow multiple clients with the same common name

        # TLS Mode Options
        tls-server          # Enable TLS and assume server role during TLS handshake
        ca ca.crt           # Certificate authority (CA) file
        dh dh1024.pem       # File containing Diffie Hellman parameters
        cert server.crt     # Local peer's signed certificate
        key server.key      # Local peer's private key
```

client.ovpn:

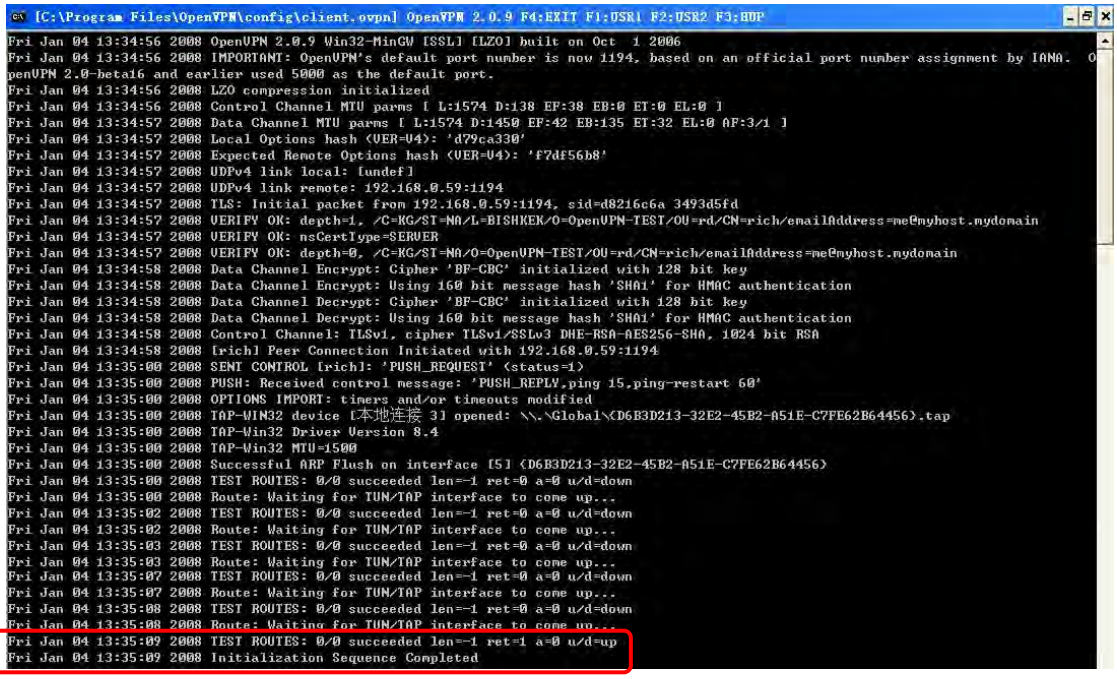
```
client
dev tap0
proto udp
remote 192.168.0.60 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
ns-cert-type server
comp-lzo
ping 15
verb 3
```

Modify according to by the router web settings

Step 3: Use the OpenVPN GUI.

(1). Open Router web page and configure the **Advanced Setting->VPN Setting->Open VPN**.

(2). In the OpenVPN Server, open "C:\Program Files\OpenVPN\config" and run server.ovpn. In the OpenVPN Client, open "C:\Program Files\OpenVPN\config" and run client.ovpn. The massage "Initialization Sequence Completed" indicates that the openvpn connection is established successfully.


[C:\Program Files\OpenVPN\config\client.ovpn] OpenVPN 2.0.9 F4:EXIT F1:USR1 F2:USR2 F3:HUP
Fri Jan 04 13:34:56 2008 OpenVPN 2.0.9 Win32-MinGW [SSL] [LZO] built on Oct 1 2006
Fri Jan 04 13:34:56 2008 IMPORTANT: OpenVPN's default port number is now 1194, based on an official port number assignment by IANA. O
penVPN 2.0-beta16 and earlier used 5000 as the default port.
Fri Jan 04 13:34:56 2008 LZO compression initialized
Fri Jan 04 13:34:56 2008 Control Channel MTU parms [L:1574 D:138 EF:38 EB:0 ET:0 EL:0]
Fri Jan 04 13:34:57 2008 Data Channel MTU parms [L:1574 D:1450 EF:42 EB:135 ET:32 EL:0 AF:3/1]
Fri Jan 04 13:34:57 2008 Local Options hash (VER=V4): 'd79ca330'
Fri Jan 04 13:34:57 2008 Expected Remote Options hash (VER=V4): 'f7df56b8'
Fri Jan 04 13:34:57 2008 UDPv4 link local: [undef]
Fri Jan 04 13:34:57 2008 UDPv4 link remote: 192.168.0.59:1194
Fri Jan 04 13:34:57 2008 TLS: Initial packet from 192.168.0.59:1194, sid=d8216c6a 3493d5fd
Fri Jan 04 13:34:57 2008 VERIFY OK: depth=1, /C=KG/ST=NA/L=BISHKEK/O=OpenVPN-TEST/OU=rd/CN=rich/emailAddress=me@myhost.mydomain
Fri Jan 04 13:34:57 2008 VERIFY OK: nsCertType=SERVER
Fri Jan 04 13:34:57 2008 VERIFY OK: depth=0, /C=KG/ST=NA/O=OpenVPN-TEST/OU=rd/CN=rich/emailAddress=me@myhost.mydomain
Fri Jan 04 13:34:58 2008 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Jan 04 13:34:58 2008 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jan 04 13:34:58 2008 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Jan 04 13:34:58 2008 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jan 04 13:34:58 2008 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Fri Jan 04 13:34:58 2008 [rich] Peer Connection Initiated with 192.168.0.59:1194
Fri Jan 04 13:35:00 2008 SENT CONTROL [rich]: 'PUSH_REQUEST' (status=1)
Fri Jan 04 13:35:00 2008 PUSH: Received control message: 'PUSH_REPLY,ping 15,ping-restart 60'
Fri Jan 04 13:35:00 2008 OPTIONS IMPORT: timers and/or timeouts modified
Fri Jan 04 13:35:00 2008 TAP-WIN32 device [本地连接 3] opened: \\.\Global\{D6B3D213-32E2-45B2-A51E-C7FE62B64456}.tap
Fri Jan 04 13:35:00 2008 TAP-Win32 Driver Version 8.4
Fri Jan 04 13:35:00 2008 TAP-Win32 MTU=1500
Fri Jan 04 13:35:00 2008 Successful ARP Flush on interface [5] {D6B3D213-32E2-45B2-A51E-C7FE62B64456}
Fri Jan 04 13:35:00 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
Fri Jan 04 13:35:00 2008 Route: Waiting for TUN/TAP interface to come up...
Fri Jan 04 13:35:02 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
Fri Jan 04 13:35:02 2008 Route: Waiting for TUN/TAP interface to come up...
Fri Jan 04 13:35:03 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
Fri Jan 04 13:35:03 2008 Route: Waiting for TUN/TAP interface to come up...
Fri Jan 04 13:35:07 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
Fri Jan 04 13:35:07 2008 Route: Waiting for TUN/TAP interface to come up...
Fri Jan 04 13:35:08 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
Fri Jan 04 13:35:08 2008 Route: Waiting for TUN/TAP interface to come up...
Fri Jan 04 13:35:09 2008 TEST ROUTES: 0/0 succeeded len=-1 ret=1 a=0 u/d=up
Fri Jan 04 13:35:09 2008 Initialization Sequence Completed